HAMPTON VA

No. IT– 053	Policy Name: Credit Card Data Protection Procedure
Effective Date: 04-01-2016 Last Revised Date: 07-29-2016	Citywide Policy_ IT Policy _ IT Procedure X
Approved By: IT Director	

Credit Card Data Protection Procedure

Scope and Purpose

All City staff members who work with credit cards and/or generate reports utilizing this data in the course of their job duties must adhere to these procedures, in order to protect sensitive credit cardholder data and comply with state, federal and payment card industry laws, regulations and standards.

References

a. Code of Virginia § 59.1-443.2 - Restricted use of social security numbers
b. Current Payment Card Industry Data Security Standards
c. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681c
   Section 605(g)(1) - Except as otherwise provided in this subsection, no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction.

Usage Guidelines and Application

All departments or entities utilizing the City as its fiscal agent and wishing to utilize credit cards for online or in person transactions shall notify the IT Department, the Finance Department and the Treasurer's Office in advance. The IT department, Finance department and the Treasurer will work with the department to ensure that proper security measures are in place to allow the processing of credit card transactions. Departments should complete a Request for Credit Card form and send it to the Treasurer, IT Director and Finance Director to start the process. The IT Department will work with the requesting department on the equipment, services and configuration to ensure security measures are in place.

Departments utilizing credit card information are responsible for ensuring that employees with access to this information understand their responsibilities in regards to this sensitive information. Security and PCI training of employees will take place at the time of hire and at least annually. The IT Department will coordinate training resources with departments.

Only employees that perform business tasks as part of their job function shall have access to physical and electronic records containing credit card information and point of sale equipment.

Department heads are required to keep a list of all employees that have access to physical or electronic credit card information. This information shall be updated as personnel changes are made.

Department heads are required to keep an up to date inventory of all point of sale devices and devices connected to a payment card system. The inventory must include the device type, brand, model, make, physical location and serial number. The IT Department may request copies of the inventory list at any time. Departments must maintain up to date manuals/documentation of all payment card readers and devices. Manuals and documentation will be kept in a secure location.

All media containing credit card information must be destroyed when it is no longer needed for business, legal or records retention purposes. Destruction must be performed as follows:

- All hardcopy materials should either be cross-cut shredded, incinerated or pulped so that the cardholder's credit card information cannot be reconstructed.
- Destruction of hardcopy materials has to be performed within 24 hours after use. Departments are encouraged to have shredding devices in close proximity to the users to encourage quick and easy destruction. Records kept longer than needed pose an unnecessary risk to citizens and the City.

The Process

All departments taking credit cards shall implement the following security measures:

- All point of sale, computers and network equipment associated with credit card payment processing will be physically secured.
    - During business hours, equipment will be behind a counter with no public access and have staff monitoring the devices at all times.
    - After hours, or when staff are not monitoring equipment, the equipment will be behind a locked door or locked in a secure area.
    - Staff will check all point of sale equipment before the start of each work day to ensure the equipment has not been tampered with and is working correctly
    - Vendors will be monitored while working on PCI equipment
    - Vendors will not be allowed to manage point of sale equipment remotely

- Other requirements for point of sale equipment
    - All point of sale equipment will be EMV compliant
    - All point of sale equipment will be configured at time of installation to not utilize the default password
    - Vulnerability scans will be conducted on networks and equipment periodically

- For Internet Connected Devices (non-dial up)
    - The City will connect PCI devices to a secure, segmented network
    - Anti-virus software will be maintained and installed systems
    - Only payment processing required software will be allowed on the device no other applications will be installed on the device
    - Generic or shared passwords will not be used
    - Critical security patches will be installed and up to date within 1 month of release
    - Only supported operating systems and hardware will be allowed
    - Advanced endpoint protection (Red Cloak) will be installed on PCs
    - Storage devices and thumb drives will not be connected to devices

All automated system, applications and manual processes shall adhere to the following procedures:

1) City employees cannot communicate in any fashion about an individual's credit card information to or in front of the general public or other employees.

2) City employees cannot print, reprint or republish an individual's full credit card number on any card or forms required for the individual to access or receive products, services or information from the City of Hampton. Exceptions shall be made only for business functions and processes requiring specific use of this information through state, federal or local mandate or law. Departments are to maintain the specific law or program requiring the use of this information and must review the use of this information annually in order to ensure full compliance with this policy.

3) Applications and systems will not require an individual to use his/her credit card number to access an Internet website. The City will deploy systems and services that require the least amount of human and system interaction with credit card numbers.

4) Applications and systems should not be sent or delivered in any letter, envelope, or package displaying a credit card number or partial credit card number on the face of the mailing envelope or package. No credit card numbers should be visible, whether on the outside or inside of the mailing envelope or package.

5) Users, applications and systems shall not send or cause the sending or delivery of any e-mail message, text message, phone message, social media or other similar technology containing a credit card number in the heading, body or attachment of messages. Partial numbers may be sent as a verifier on an exception basis and shall be approved by the IT Director and the City Attorney's Office if in compliance with Paragraph 7 below. Users, applications and systems should make every effort to avoid the use of even partial displays of card numbers.

6) No users, applications or systems used by the COH shall embed an encrypted or unencrypted credit card number in or on a card or document. This includes, but isn't limited to, using a bar code, chip, magnetic strip, or other technology.

7) All applications, systems and manual documents produced by the COH shall mask the credit card number when displayed. The last four digits are the maximum number of digits to be displayed for credit card information. The card verification code or value (three or four-digit number printed on the front or back of the payment card) shall not be stored under any circumstances.

8) The personnel identification number (PIN) of the encrypted PIN block cannot be stored under any circumstances.

9) If a City employee discovers that a credit card number has been released by a fellow COH employee to anyone besides the intended party, the following steps shall be taken:

   a) Notify their immediate supervisor and department head of the date, time and incident description as soon as the incident is discovered.

   b) The immediate supervisor or department head must contact the City Attorney's office immediately and receive instructions on how to proceed with the incident.

Additional Documents/ Forms

1. Department Credit Card Request